



Azure 모니터링

한국마이크로소프트 박인혜

# Azure 모니터링

Service Health/Azure 모니터/Log Analytics

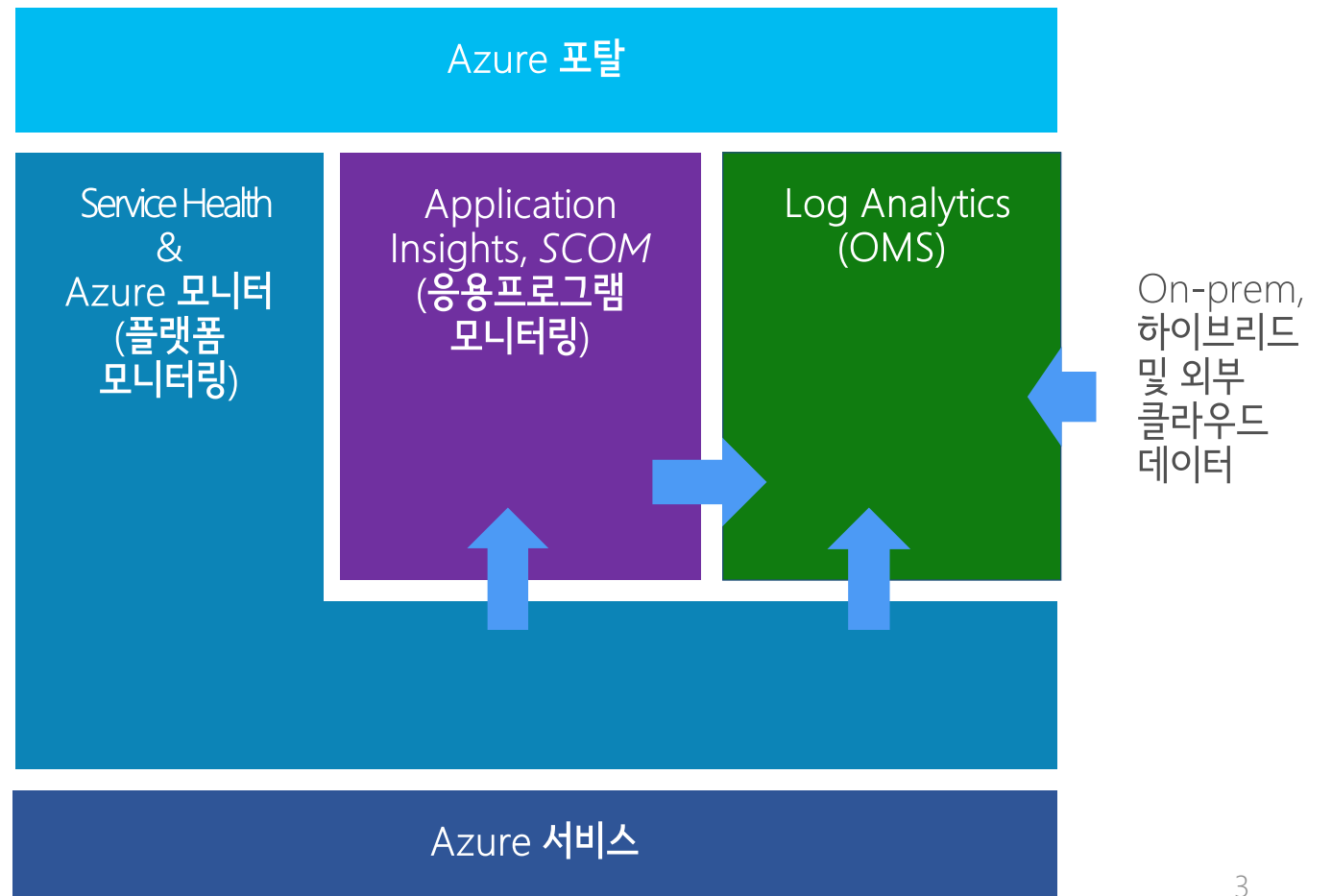
# Agenda

- Service Health
- Azure **모니터**
- Log Analytics(OMS)

REST API, 이벤트 허브,  
스토리지 로그 파일을 통해  
3rd party 제품 연동



## Azure 서비스에 대한 End-to-End 모니터링 환경

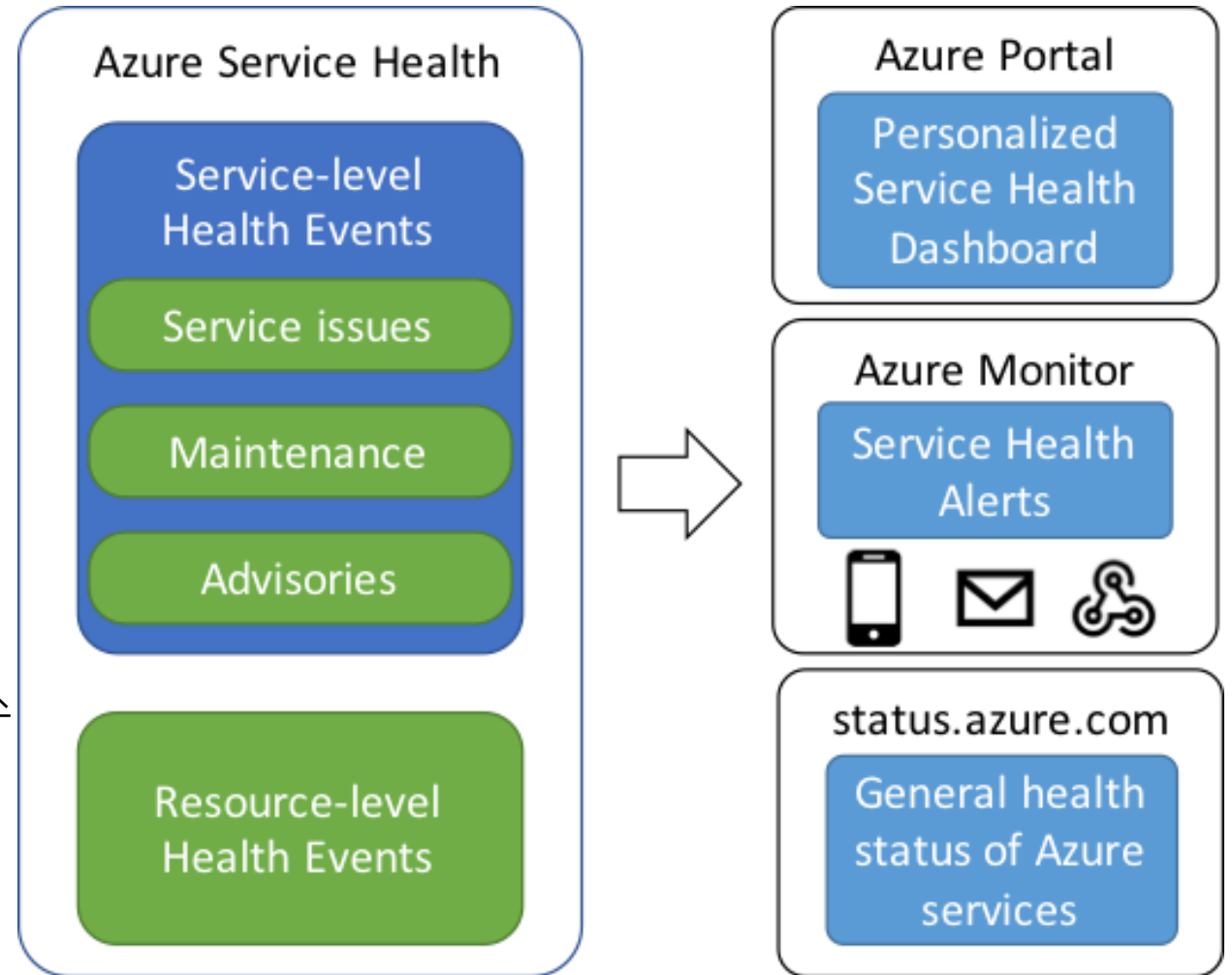


Service Health



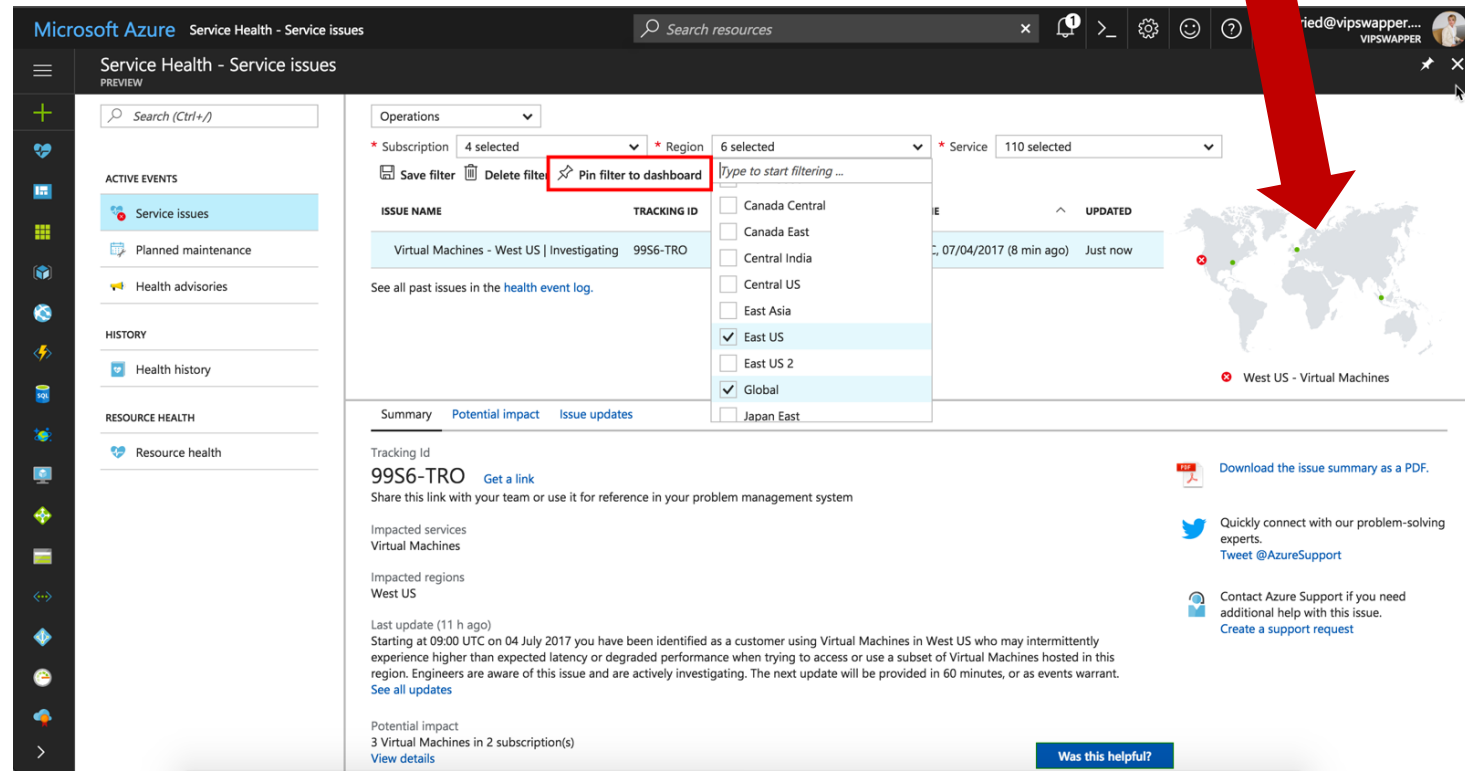
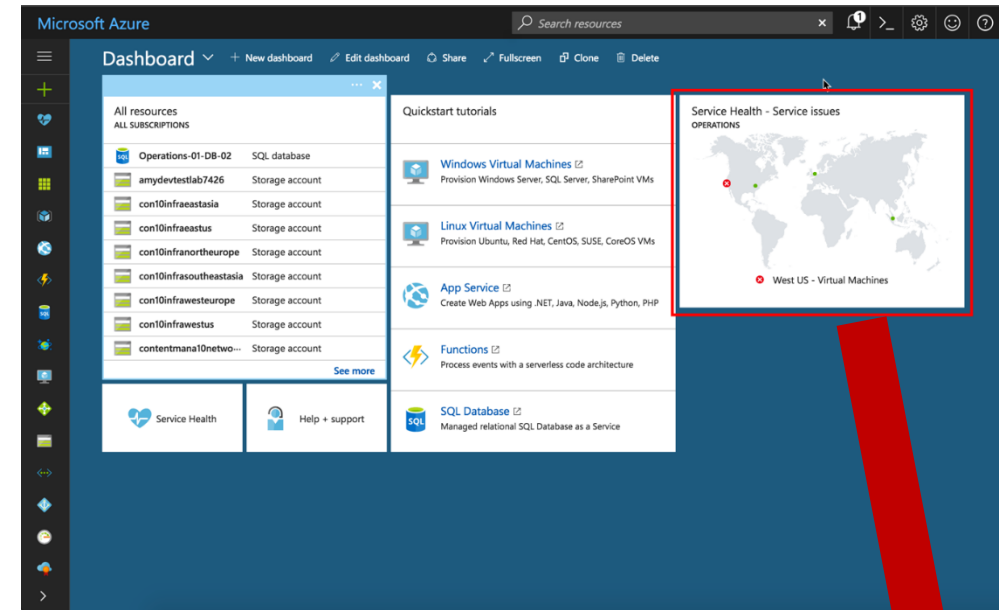
# 서비스 상태(Service Health)

- Azure 서비스의 상태 정보를 제공
- 상태 데이터 출처 : <https://azure.microsoft.com/en-us/status/>
- 리소스에 영향을 줄 수 있는 다음 세 가지 유형의 상태 이벤트를 추적
  - **서비스 문제(Service issues)** – 고객에게 당장 영향이 있을 수 있는 Azure 서비스 상의 문제
  - **계획된 유지 관리(Planned maintenance)** – 향후 서비스 가용성에 영향을 줄 수 있는 예정된 유지보수 작업
  - **상태 공지(Health advisories)** – 고객 주의가 필요한 Azure 서비스 상의 변경 사항. 일례로 향후 더이상 지원하지 않는 기능이 있거나, 할당된 사용량을 초과한 경우에 해당



# 서비스 문제(Service Issue)

- 고객 리소스에 영향을 줄 수 있는 Azure 서비스 상의 지속되고 있는 문제를 보여줌
- 구독/서비스 지역/이벤트/기간 범위 기반 필터링 지원
- 사후 정보 제공



# 리소스 상태(Resource Health)

- Azure 리소스의 상태 정보 제공
- 리소스가 정상인지를 판별하기 위해 Azure 서비스에 의해 발생한 다양한 시그널을 참조
- Resource Health는 다음 중 하나의 상태를 제시
  - **사용 가능(Available)** – 리소스 상태에 영향을 주는 어떠한 이벤트도 발생하지 않았음
  - **사용할 수 없음(Unavailable)** – 리소스 상태에 현재 영향을 주고 있는 플랫폼 또는 비플랫폼 기반의 이벤트를 탐지
  - **알 수 없음(Unknown)** – 10분 이상 해당 리소스에 대해 상태 정보를 전달받지 못함

홈 > 모니터 > 서비스 상태 - Resource Health

### 서비스 상태 - Resource Health

검색(Ctrl+/)

활성 이벤트

- 서비스 문제
- 계획된 유지 관리
- 상태 공지 (1)

기록

- 상태 기록

리소스 상태

- Resource Health

경고

- 상태 경고

구독 ⓘ

inpa

리소스 이름	형식
aks-agentpool-34725021-0	가상 머신
aks-agentpool-34725021-1	가상 머신
aks-agentpool-34725021-2	가상 머신
cosmos-win	가상 머신
cosmosDev	가상 머신
k8s-agent-498D7AA8-0	가상 머신
k8s-agent-498D7AA8-1	가상 머신
k8s-agent-498D7AA8-2	가상 머신
k8s-master-498D7AA8-0	가상 머신
monitor-vm01	가상 머신
monitorwin	가상 머신
MSFT-AMS-VM01	가상 머신
node1	가상 머신
node2	가상 머신
node3	가상 머신

리소스 종류 ⓘ

가상 머신

- IoT Hub
- Log Analytic
- Machine Learning Studio 웹 서비스
- Managed database
- Power BI Embedded
- Power BI 작업 영역 컬렉션
- Redis Cache
- SQL 데이터베이스
- Search 서비스
- Traffic Manager 프로필
- VPN 게이트웨이
- VPN 연결
- 가상 머신
- 가상 머신(클래식)
- 문서 DB
- 미디어 서비스
- 부하 분산 장치
- 서비스 버스
- 서비스 팩트릭 클러스터
- 스트림 분석 작업
- 알림 허브 네임스페이스
- 웹 사이트
- 저장소 계정
- 키 자격 증명 모음

# 리소스 상태(Resource Health)

- API를 통해 접근 가능
- 기록 정보를 최대 14일까지 제공

- Resource health의 지원 리소스 타입 및 상태 검사 항목 :

<https://docs.microsoft.com/en-us/azure/service-health/resource-health-checks-resource-types>

demoapimanagementservice - 리소스 상태		
API Management 서비스		
검색(Ctrl+/)	새로 고침	
리소스		
설정		
속성		
규모 및 가격 책정		
Virtual network		
SSL		
사용자 지정 도메인		
관리 서비스 ID		
잠금		
자동화 스크립트		
모니터링		
Application Insights		
경고		
메트릭		
진단 설정		
로그		
지원 및 문제 해결		
리소스 상태		
12/13/2018	✓ 사용 가능	
12/12/2018	✓ 사용 가능	
12/11/2018	✓ 사용 가능	
12/10/2018	✓ 사용 가능	
12/09/2018	✓ 사용 가능	
12/08/2018	✓ 사용 가능	
▼ 12/07/2018	! 4 상태 이벤트	
09:50 (GMT+9) - 09:50 (GMT+9)	? 현재 이 API Management 서비스의 상태를 확인할 수 없습니다.	
09:31 (GMT+9) - 09:32 (GMT+9)	? 현재 이 API Management 서비스의 상태를 확인할 수 없습니다.	
09:02 (GMT+9) - 09:04 (GMT+9)	? 현재 이 API Management 서비스의 상태를 확인할 수 없습니다.	
00:00 (GMT+9) - 07:21 (GMT+9)	! API Management 서비스를 최신 버전으로 업그레이드하는 중입니다.	
▶ 12/06/2018	! 4 상태 이벤트	
12/05/2018	✓ 사용 가능	
▶ 12/04/2018	! 1 상태 이벤트	
12/03/2018	✓ 사용 가능	



Azure 모니터

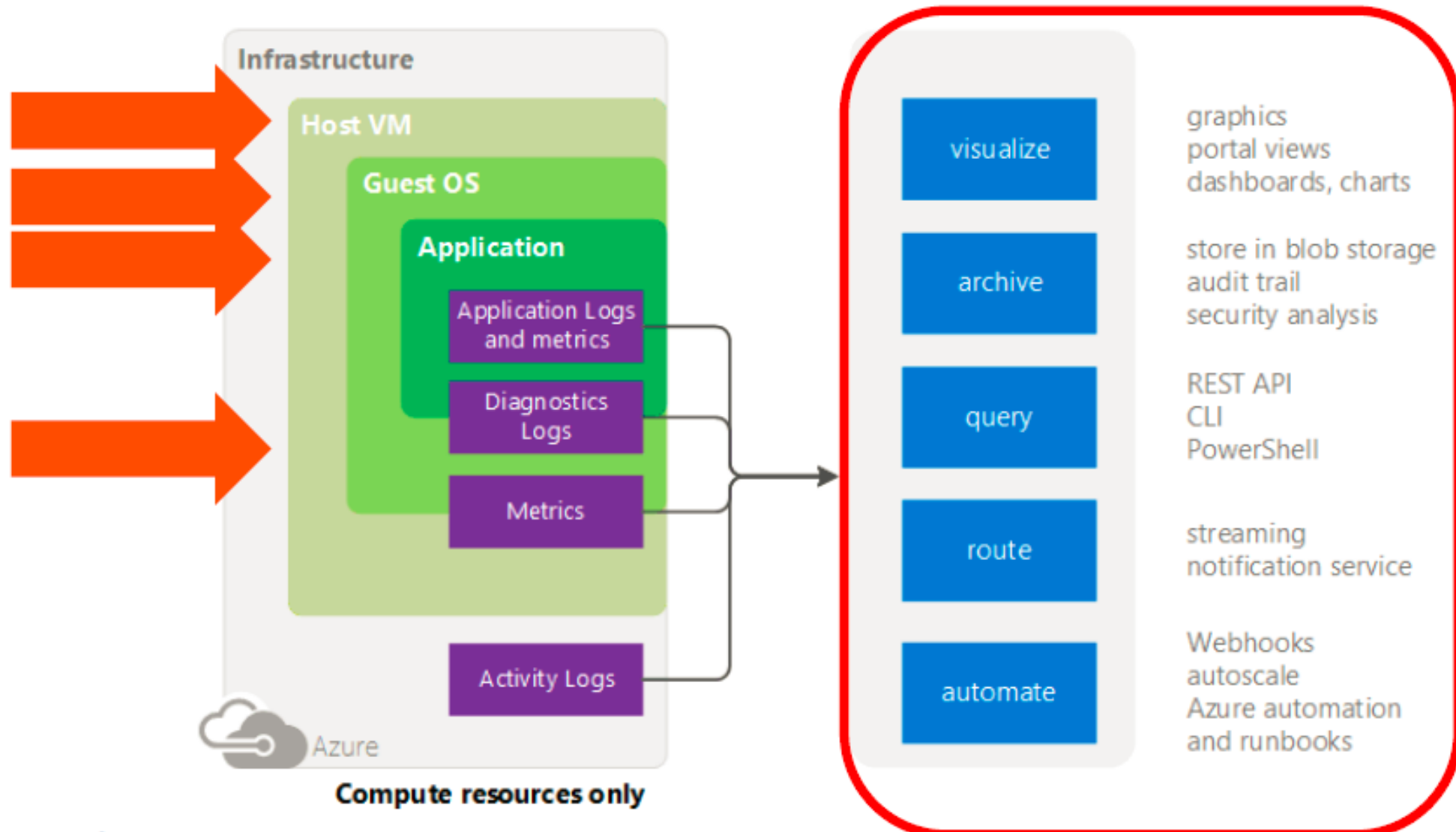
# Azure 모니터

- Azure 리소스에 대한 자체 제공 모니터링 기능
- 메트릭 및 로그 기반
- 알림을 받거나 & 자동화된 작업을 수행할 경고 규칙
- 플랫폼 및 어플리케이션 모니터링을 위한 단일 대시보드
- 3rd party 연계를 위한 API

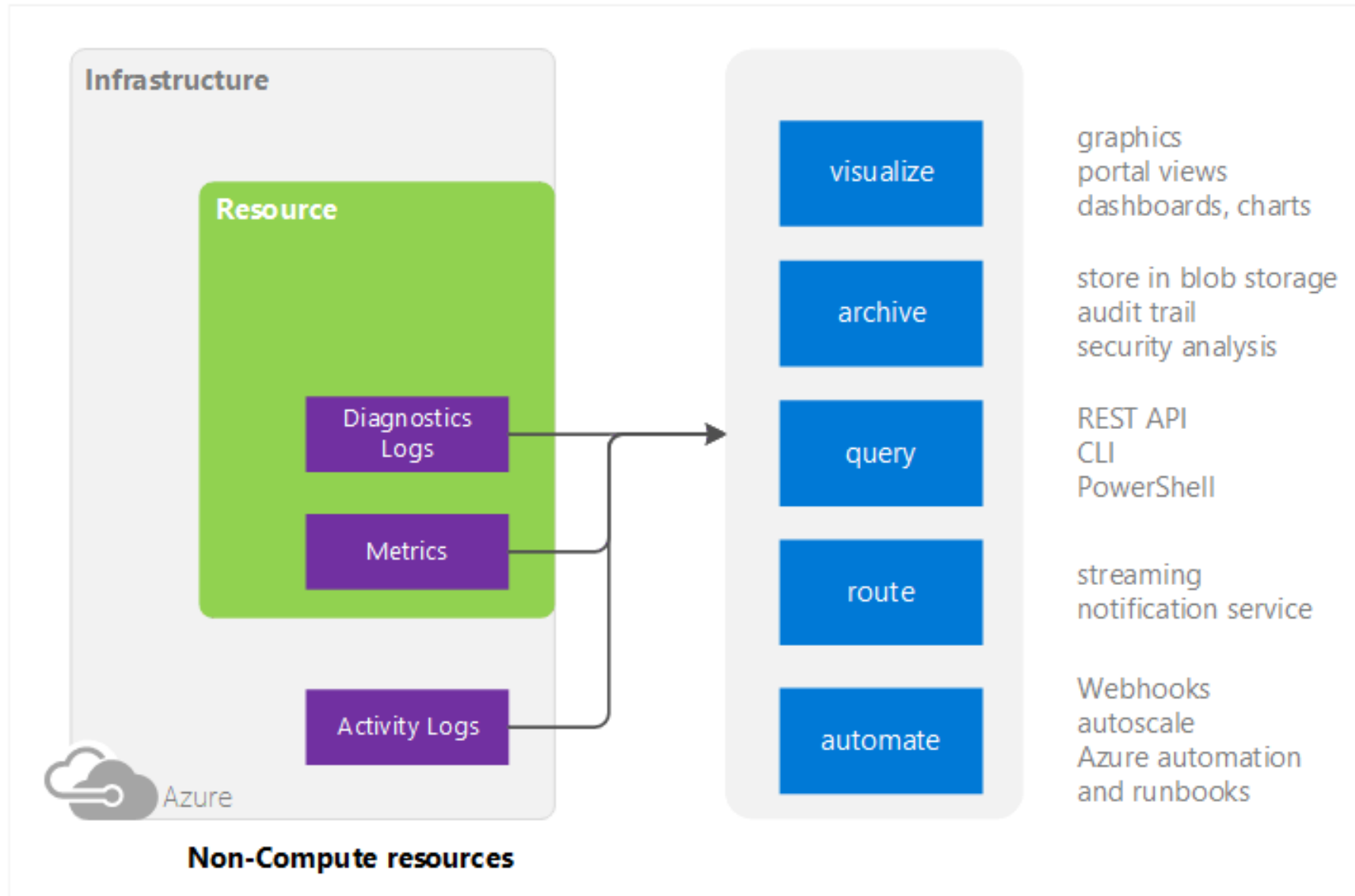
# Azure 모니터에서 수집되는 데이터

- 응용 프로그램 모니터링 데이터
  - ✓ 플랫폼에 관계없이, 작성한 코드의 성능 및 기능에 대한 데이터
- 게스트 OS 모니터링 데이터
  - ✓ 응용 프로그램이 실행되고 있는 운영 체제에 대한 데이터
  - ✓ Azure, 다른 클라우드 또는 온-프레미스에서 실행될 수 있음
- Azure 리소스 모니터링 데이터
  - ✓ Azure 리소스의 작업에 대한 데이터
- Azure 구독 모니터링 데이터
  - ✓ Azure 구독의 운영 및 관리에 대한 데이터와 Azure 자체의 상태 및 작업에 대한 데이터
- Azure 테넌트 모니터링 데이터
  - ✓ Azure Active Directory 등, 테넌트 수준 Azure 서비스의 작업에 대한 데이터

# Azure 모니터 – Compute Resources Only



# Azure 모니터 – Non-Compute Resources





# 리소스 로그

## 활동 로그

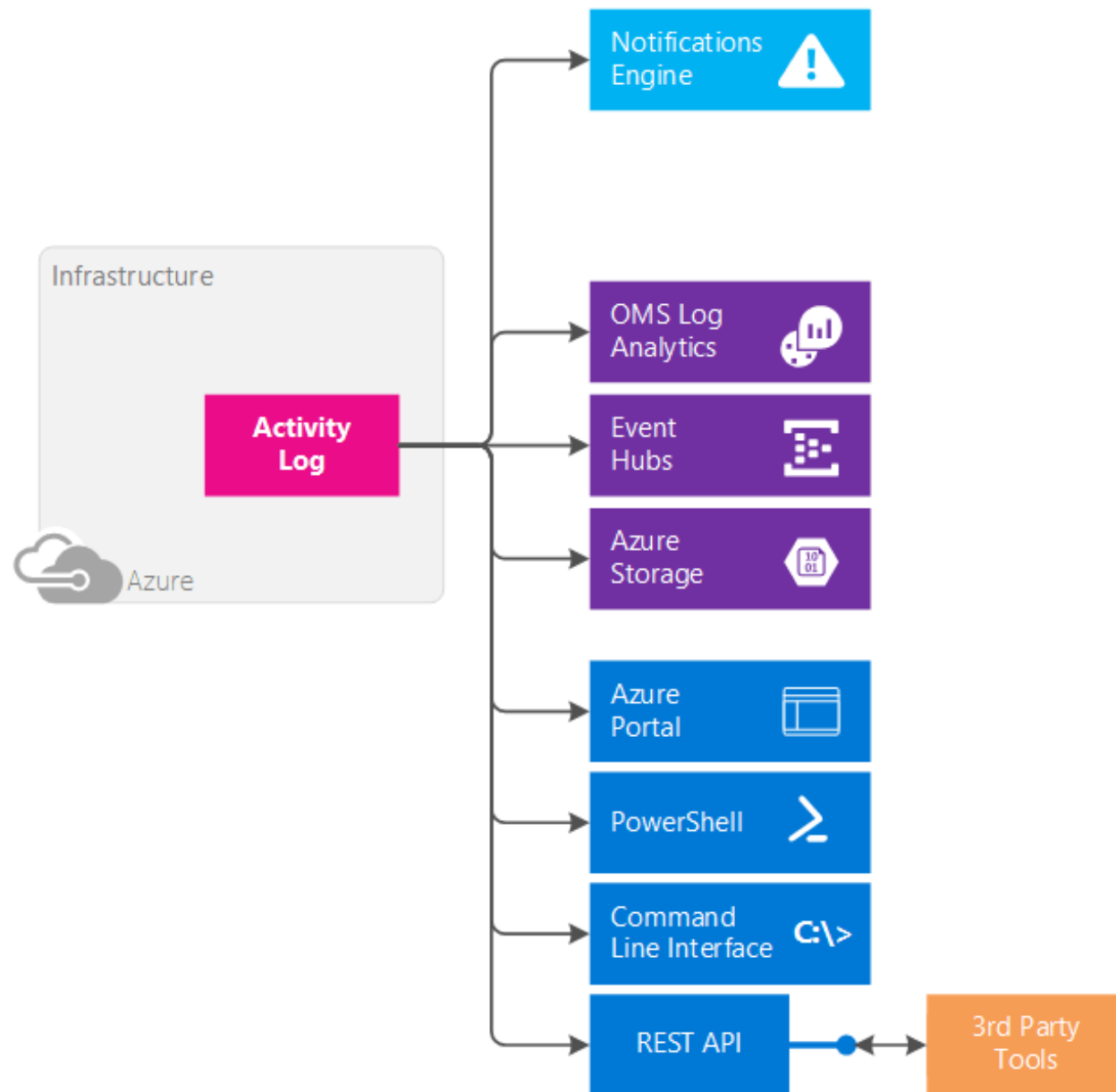
- 감사 로그로도 일컬어 짐
- 운영 상세를 기록
- Azure 상에서 누가, 언제, 무엇을 했는지에 대한 정보 제공
- 예) 가상 컴퓨터 만들거나 논리 앱 삭제 등, Resource Manager를 사용하여 구독에서 리소스에 대해 수행된 작업에 대한 정보를 제공

## 진단 로그

- 이벤트 로그 (시스템, 응용 프로그램, 보안)
- IIS 로그
- 크래시 덤프 데이터
- 사용자 지정 에러 로그
- 성능 카운터  
(➔ 대부분은 Azure 메트릭에 의해 처리 됨 )

# 활동 로그

- 리소스들에 대한 관리 작업 로그들을 포함  
(=누가 언제, 어떤 리소스에 무엇을 하였나?)
- Azure 포털 또는 REST API를 통해 사용
- Blob 저장소로 내보내기 또는 Event Hub로 스트리밍
- Log Analytics 기반의 내장된 검색 및 분석 기능
- 이벤트로부터 이메일 또는 Webhook 트리거 생성
- 활동 로그 이벤트 스키마 :  
<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-activity-log-schema>



# 활동 로그

홈 > 모니터 - 활동 로그

## 모니터 - 활동 로그

Microsoft

🔍 검색(Ctrl+/)

📊 개요

📅 활동 로그

⚠️ 경고

📈 메트릭

📊 로그

🏥 Service Health

인사이트

💡 응용 프로그램

🖥️ Virtual Machines(미리 보기)

🔗 컨테이너

🌐 네트워크

⋮ 자세히

☰ 열 편집

🔄 새로 고침

📤 이벤트 허브로 내보내기

⬇️ CSV로 다운로드

📄 로그

📌 현재 필터 고정

🔄 필터 재설정

🔍 검색

✕

💡 빠른 인사이트 활용

구독 : inpa

시간 간격 : 지난 6시간

이벤트 심각도 : 모두

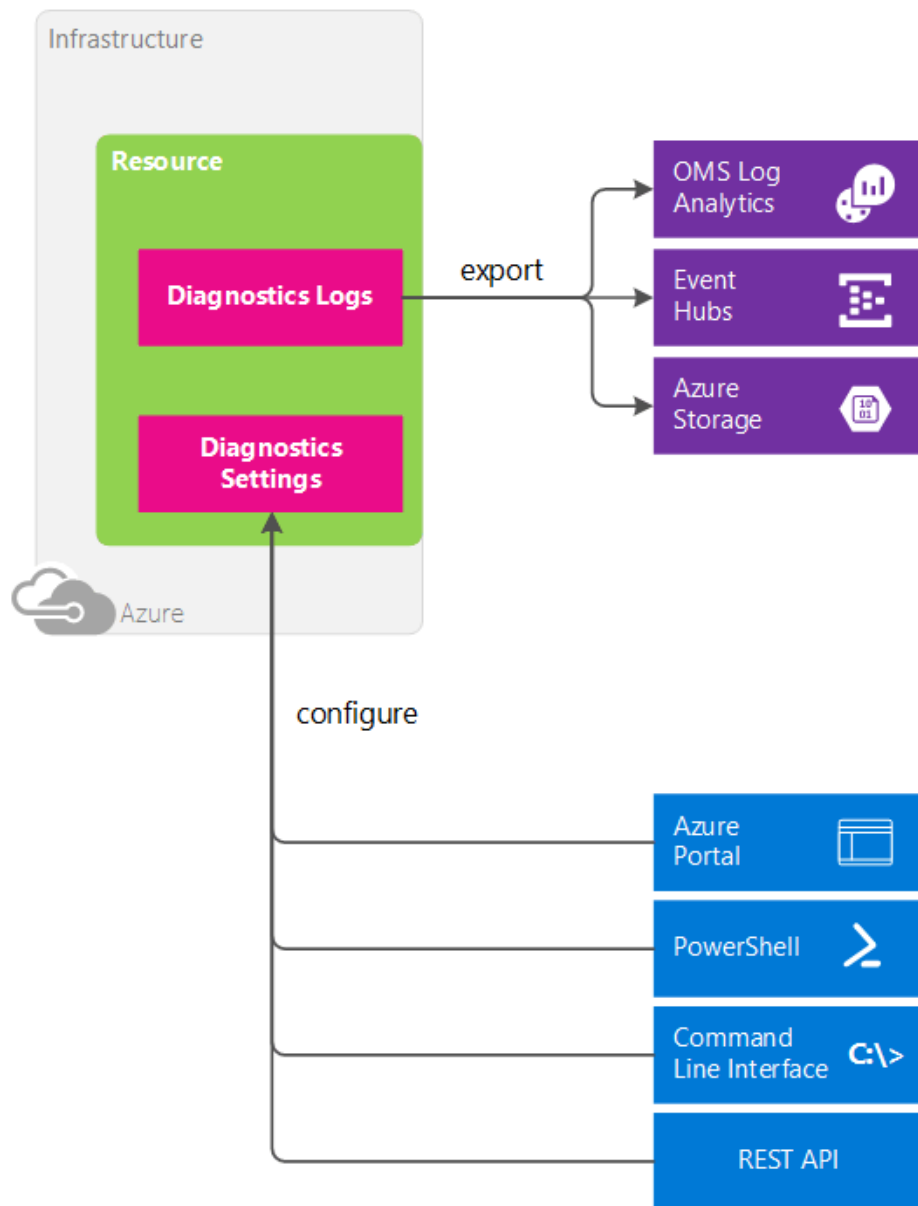
+🔍 필터 추가

98개 항목입니다.

작업 이름	상태	시간	타임스탬프	구독	이벤트를 시작한 사람
▶ ⓘ Register with the Provider	성공	32분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com
▶ ⓘ Register with the Provider	성공	36분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com
▶ ⓘ Get SSO token	성공	36분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com
▼ ⓘ Create or Update Virtual Machine Extension	성공	39분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com
ⓘ Create new OMS solution	시작	53분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com
ⓘ Create new OMS solution	시작	52분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com
ⓘ Create Workspace	시작	52분 전	Mon Dec 17 20...	inpa	inpa@microsoft.com

# 진단 로그

- 단일 위치에서 진단로그 설정을 관리
- 리소스 유형 별로 로그 콘텐츠가 상이
- 로깅은 별도 활성화가 필요
- 보관 또는 오프라인 보고를 위한 Blob 저장소
- 커스텀 앱 또는 3rd party 연계를 위해 Event Hub로 스트리밍
- 고급 분석을 위해 Log Analytics 로 전달
- Azure 진단 로그 관련  
지원 서비스, 스키마 및 카테고리 :  
<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-diagnostic-logs-schema>



# 진단 로그

홈 > 모니터 - 진단 설정

모니터 - 진단 설정

Microsoft

검색(Ctrl+/)

개요

활동 로그

경고

메트릭

로그

Service Health

인사이트

응용 프로그램

Virtual Machines(미리 보기)

컨테이너

네트워크

자세히

설정

새로 고침

구독

리소스 그룹

리소스 종류

리소스

inpa

입력하여 필터링 시작...

0개 선택됨

입력하여 필터링 시작...

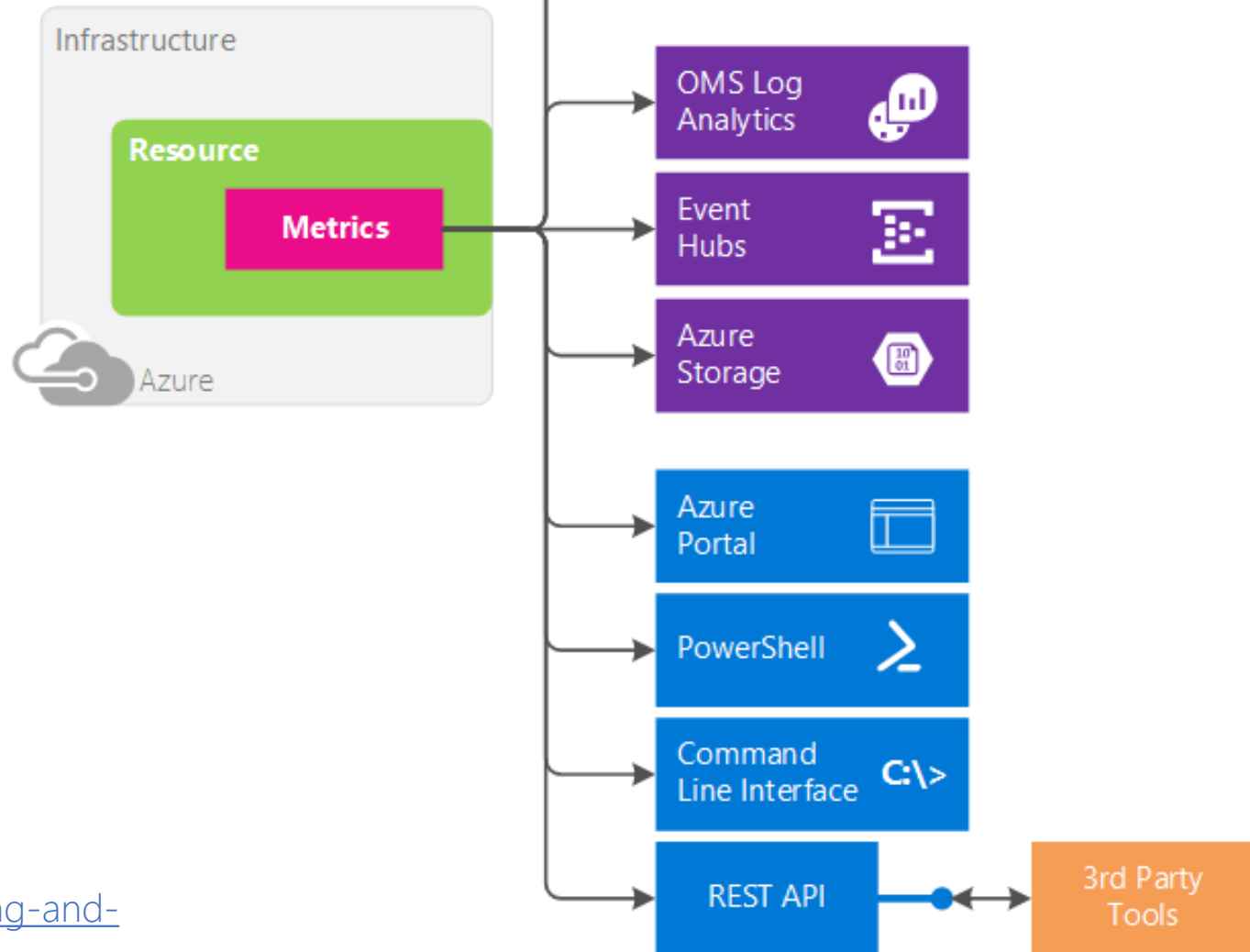
로그를 볼 리소스를 선택하세요.

이름	리소스 종류	리소스 그룹	진단 상태
opgg-kubenet	Kubernetes 서비스	container-rg	사용
cosmos-win-nsg	네트워크 보안 그룹	cosmos-dev-rg	사용 안 함
cosmosDev-nsg	네트워크 보안 그룹	cosmos-dev-rg	사용 안 함
cosmos-win-ip	공용 IP 주소	cosmos-dev-rg	사용 안 함
cosmosDev-ip	공용 IP 주소	cosmos-dev-rg	사용 안 함
DemoLogicApp	논리 앱	Demo	사용 안 함
devopsappmysqlserver	Azure Database for MySQL 서버	devopsairlift-rg	사용 안 함
cosmos-win-nsg	네트워크 보안 그룹	devopsairlift-rg	사용 안 함



# 메트릭 (Performance counters)

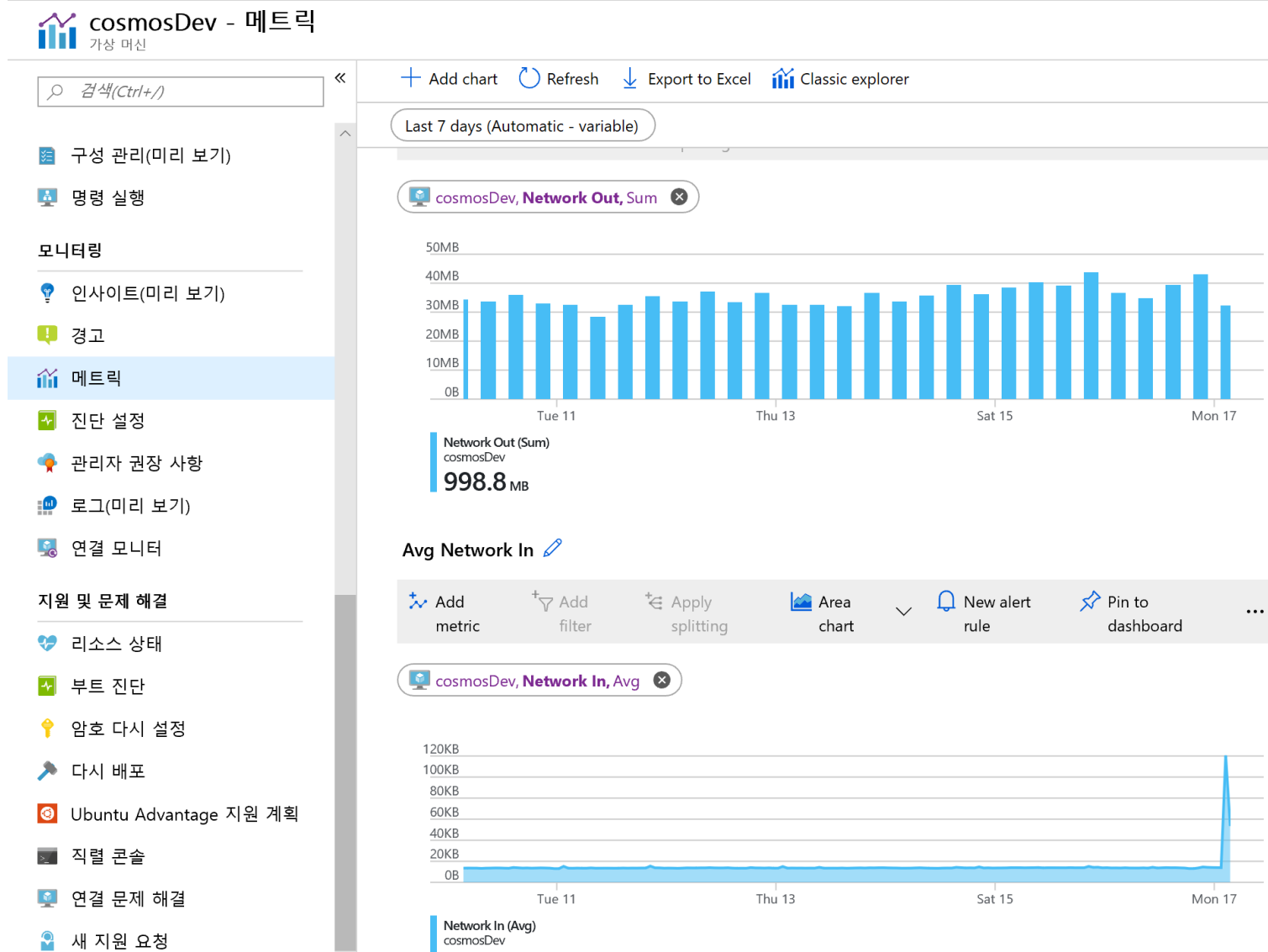
- 1분 단위 / 93일 기준 데이터 보존
- 진단 설정(또는 스토리지 계정)이 필요 없음 – Azure 가상 머신 기준으로 호스트 메트릭만 지원
- Azure 가상 머신 게스트 운영 체제(Guest-OS) 메트릭에 대해서는 Azure 확장이 요구됨
- Blob 저장소, Azure Event Hub 또는 OMS로 내보내기
- Azure 포털 또는 REST API를 통해 사용
- 메트릭에 대한 경고 규칙 구성
- Azure Monitor에 대해 지원되는 metric :  
<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics>



# 메트릭 데이터의 원본(Sources of metric data)

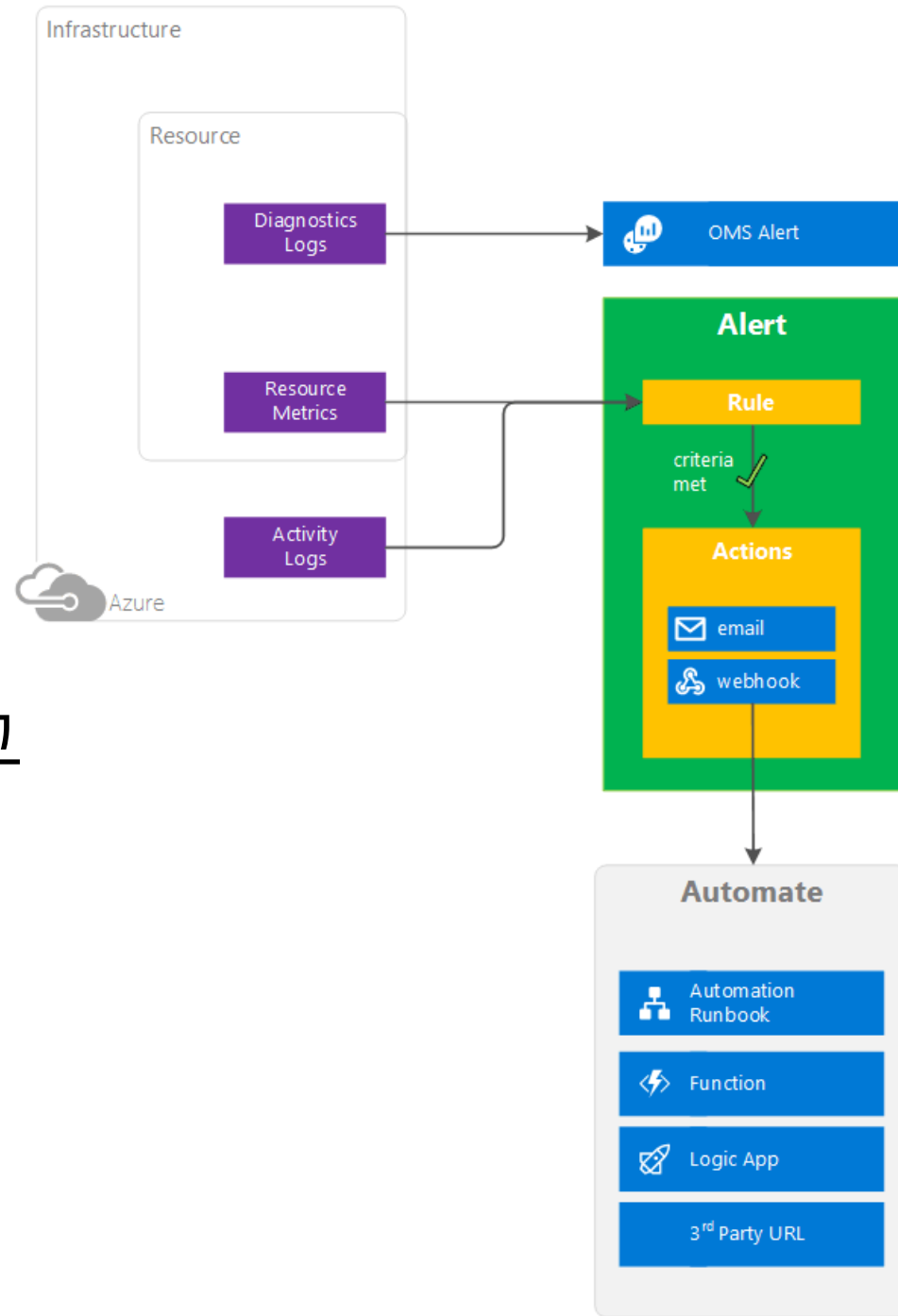
- 플랫폼 메트릭
  - ✓ Azure 리소스에서 생성되고 해당 상태 및 성능에 대한 가시성을 제공
  - ✓ 각 리소스 유형은 필요한 구성 없이 고유 메트릭 집합으로 구성
- 응용 프로그램 메트릭
  - ✓ 모니터링된 응용 프로그램에 대한 Application Insights에 의해 생성
  - ✓ 성능 문제를 감지
  - ✓ 응용 프로그램이 사용되는 추세를 추적
  - ✓ 예) 서버 응답 시간 및 브라우저 예외
- 사용자 지정 메트릭
  - ✓ 자동으로 사용할 수 있는 표준 메트릭 외에 정의하는 메트릭
  - ✓ 해당 리소스와 동일한 지역에서 단일 리소스에 대해 생성되어야 함
  - ✓ Application Insight, Windows 진단 확장(WAD), InfluxData Telegraf 에이전트, 사용자 지정 메트릭 API를 사용하여 구현

# 플랫폼 메트릭 (Performance counters)



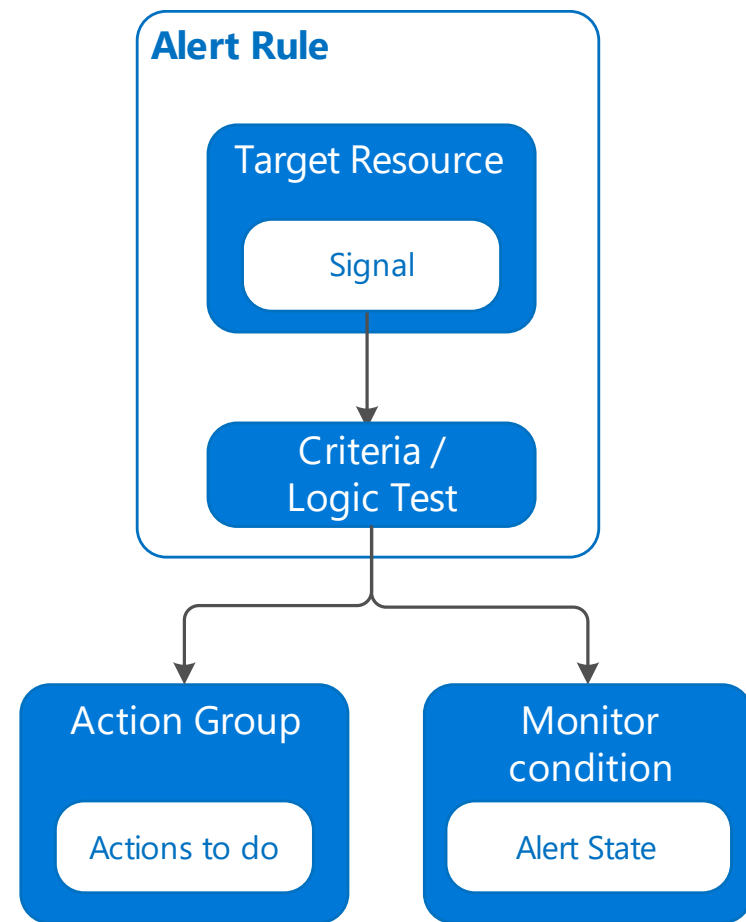
# 경고

- 단일 위치에서 모든 경고를 관리
- 이메일 및 Webhook 알림을 통해 플랫폼, 앱 그리고 커스텀 메트릭에 대한 경고 제공
- 활동 로그와 Service Health 알림에 대한 경고
- 재사용 가능한 *Notification Groups* 을 활용한 더 나은 경고 관리



# 경고

- 경고 규칙 - 경고 규칙은 경고의 대상 및 조건
- 대상 리소스 - 가상 머신, 스토리지 계정, 가상 머신 확장 집합, Log Analytics 작업 영역 또는 Application Insights 리소스 등
- 신호 - 메트릭, 활동 로그, Application Insights 및 로그
- 조건 - 예) 백분율 CPU 70% 이상, 서버 응답 시간 4ms 이내, 로그 쿼리의 결과 수 100개 이상
- 경고 이름 - 사용자가 구성한 경고 규칙의 구체적인 이름
- 경고 설명 - 사용자가 구성한 경고 규칙의 설명
- 심각도 - 경고 규칙에 지정된 조건이 충족될 때의 경고 심각도. 심각도 범위는 0~4





# 경고

## 활동 로그 경고

### 규칙 만들기

규칙 관리



#### \* 리소스

계층 구조



cosmos-win/Microsoft.Insights.VMDiagnosticsSettings



inpa



cosmos-dev-rg

선택



#### \* 조건



다음과 같을 때마다: 관리 작업 로그 "Create or Update Virtual Machine Ex...



조건 추가



현재 경고 규칙당 2개의 메트릭 신호, 1개의 로그 검색 신호 또는 1개의 활동 로그 신호 구성만 지원합니다. 위에 구성된 모든 기준의 조건이 충족되면 경고가 트리거됩니다.



#### \* 작업 그룹

이메일 및 문자 메시지를 통해 팀에 알리거나 웹훅, Runbook, Functions, Logic Apps를 사용하여 작업을 자동화하거나, 외부 ITSM 솔루션과 통합하세요. 자세한 정보 [여기](#)

작업 그룹 이름

작업 그룹 유형

ActivityLogAlerts

기존 항목 선택

새로 만들기

경고 규칙 만들기

## 메트릭

### Metric

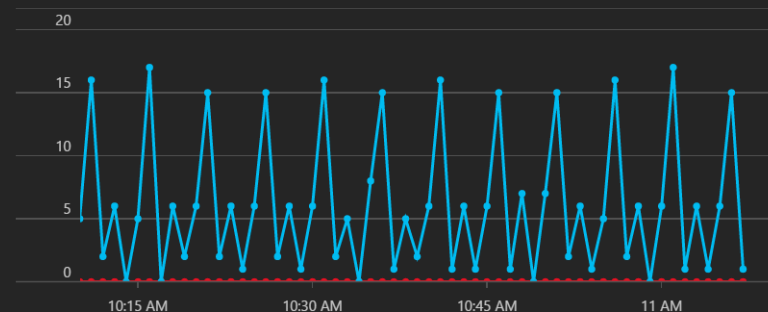
loanapp2

+ Add alert

Dagnostic sett...

Edit chart

#### Requests and errors



REQUESTS

351

HTTP SERVER ERRORS

0

METRIC	AVERAGE	MINIMUM	MAXIMUM	TOTAL
Http Server Errors	0	0	0	0
Requests	6.05	0	17	351

#### Alerts

NAME	CONDITION	LAST ACTIVE
LOANAPP2 (SITES) (SELECTED METRICS)		
ServerErrors loanapp2	Erros do Servidor Http > 0 Cou...	Never
LOANAPP2 (SITES) (ALL OTHER METRICS)		

# 문제 진단 및 해결

- Resource Health
- 최근 활동
- 일시적인 문제에 대한 해결 방법
- 도구
- Microsoft 지원에 문의

cosmos-win - 문제 진단 및 해결  
가상 머신

검색(Ctrl+/)

개요

활동 로그

액세스 제어(IAM)

태그

문제 진단 및 해결

설정

네트워킹

디스크

크기

보안

확장

지속적인 업데이트(미리 보기)

가용성 집합

구성

ID

속성

잠금

자동화 스크립트

작업

자동 종료

백업

재해 복구

업데이트 관리

인벤토리

변경 내용 추적

Resource Health

마지막으로 확인한 날짜 2018. 12. 17. 오전 4:31:21

Available

이 가상 머신에 영향을 주는 것으로 알려진 Azure Platform 문제가 없습니다. [자세히](#)

최근 활동

지난 24시간 동안의 활동

[빠른 인사이트 활용](#) | [모든 활동 보기](#)

일반적인 문제에 대한 해결 방법

▽ I can't connect to my Windows VM

▽ I can't create or add a VM

▽ I can't restart or resize an existing VM

▽ I can't connect to an application on my VM

▽ My VM is slow

▽ My VM restarted unexpectedly

▽ I could not enable Update Management, Change Tracking and Inventory, or Desired State Configuration

▽ My issue is not listed

도구

[암호 다시 설정](#)  
기본 제공 관리자 계정의 암호 다시 설정

직렬 콘솔

Virtual Machines 직렬 콘솔에 로그인

부트 진단 보기  
시작 문제를 진단하기 위해 이 가상 머신의 직렬 콘솔 출력 및 스크린샷을 봅니다. 가상 머신의 지원 및 문제 해결이라는 하위 머리글 아래에서 부트 진단 메뉴 항목을 선택하여 액세스할 수 있습니다.

[가상 머신 다시 배포](#)  
연결 문제를 해결하기 위해 이 가상 머신을 다른 호스트로 마이그레이션

Microsoft 지원에 문의

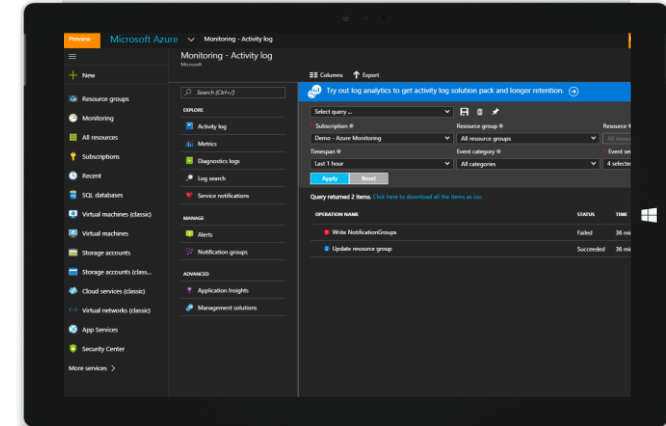
문제를 해결하기 위한 지원이 필요하다면 다음을 여세요. [지원 요청](#)

# 모니터 - 요약

모든 모니터링, 진단, 경고,  
알림에 대한 손쉬운 검색 및  
중앙화된 접근

플랫폼 리소스 메트릭, 1분  
단위, 93일 보존, 설정 불필요,  
항상 사용 가능함

플랫폼, 앱, OMS 솔루션,  
보안 등 모든 것을  
모니터링하기 위한 단일  
대시보드



## Azure Monitor

커스텀 및 응용 프로그래  
메트릭을 위한 Application  
Insights과의 연동

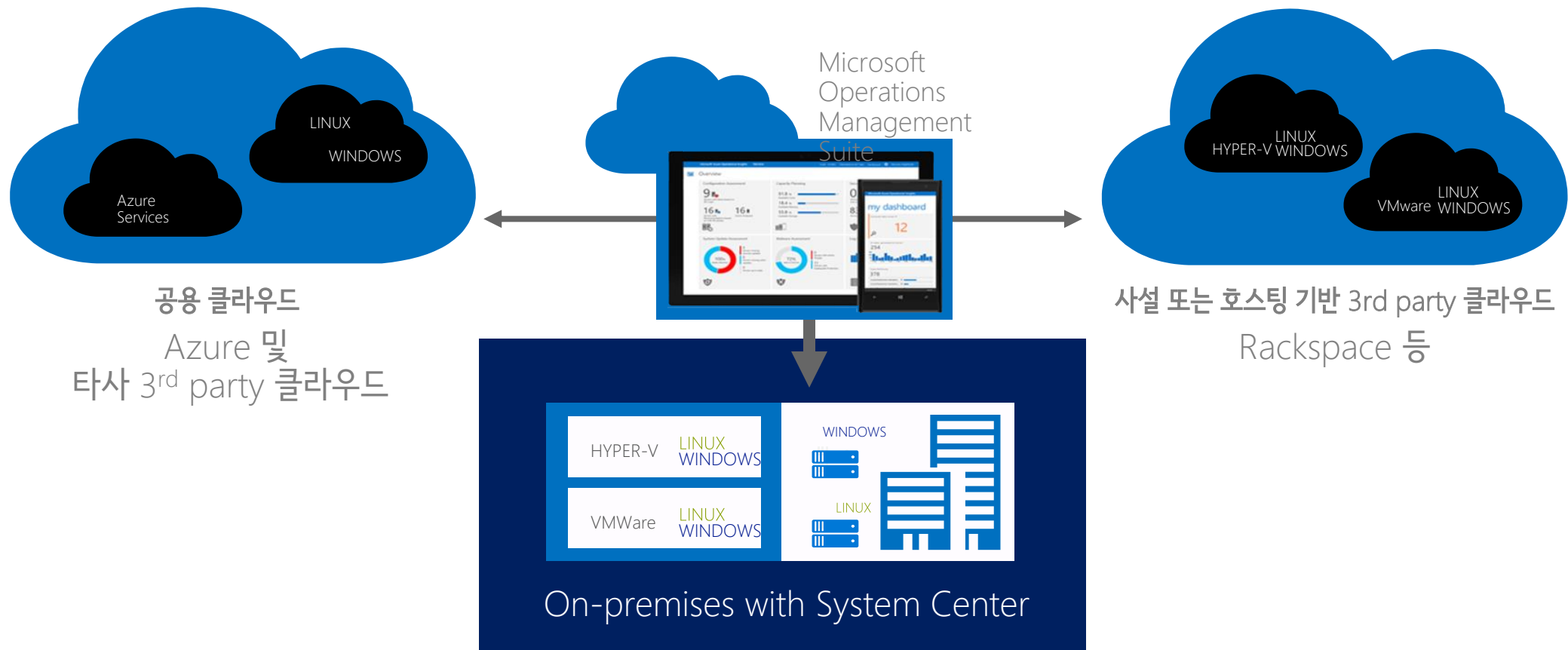
Log Analytics 기반으로 구독 간  
로그 분석

풍부한 에코시스템 바탕으로 파트너  
모니터링 도구와의 직접적인 연계

Log Analytics(OMS)

# Operations Management Suite (OMS)

- 온-프레미스 및 클라우드 모두에 대해 간소화된 게스트 및 워크로드 관리

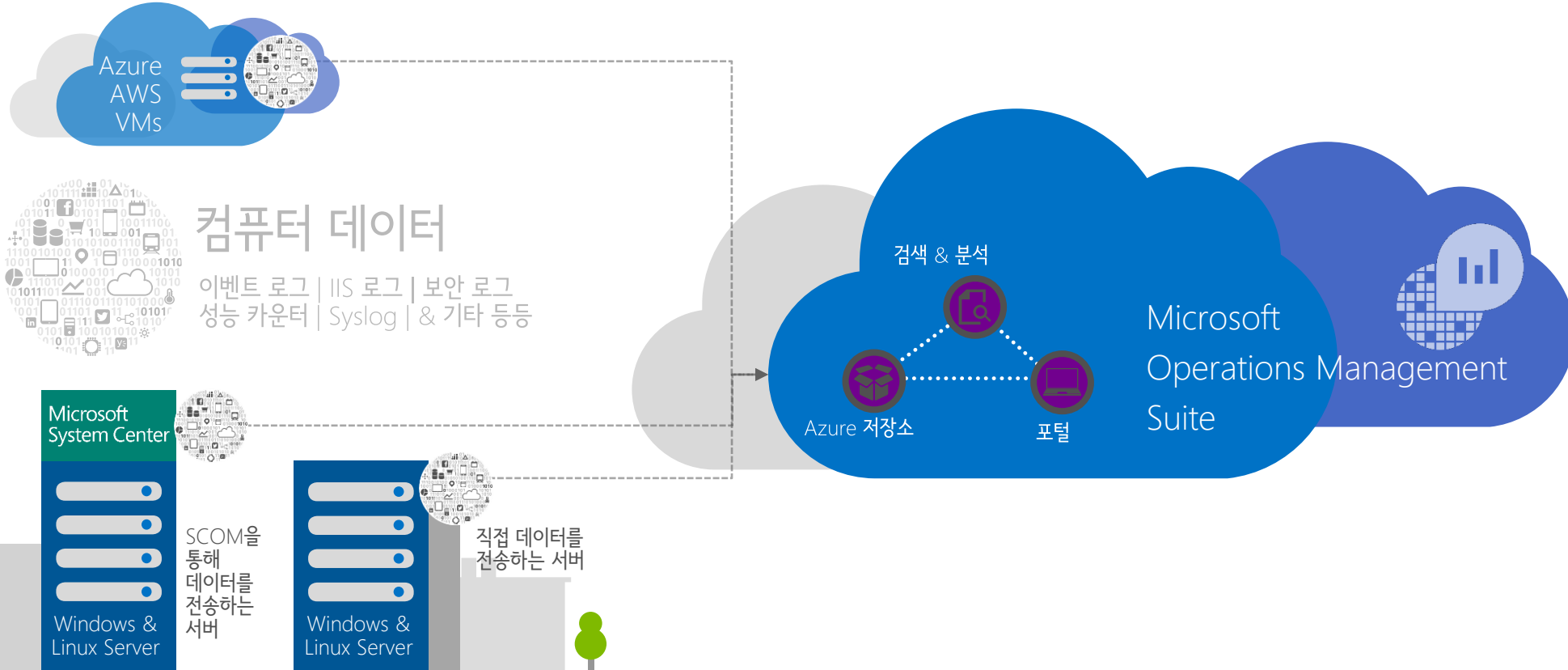






# Log Analytics 서비스

로그 분석으로 기업에서 컴퓨터 데이터를 실시간에 가까운 운영 인텔리전스로 변화



로그 관리  
여러 데이터 소스  
작업 컨텍스트  
시스템 평가  
용량 예측  
변경 추적  
규정 준수 확인  
System Center 통합



실시간, 유연한 크기조정



검색, 상관관계 & 결합



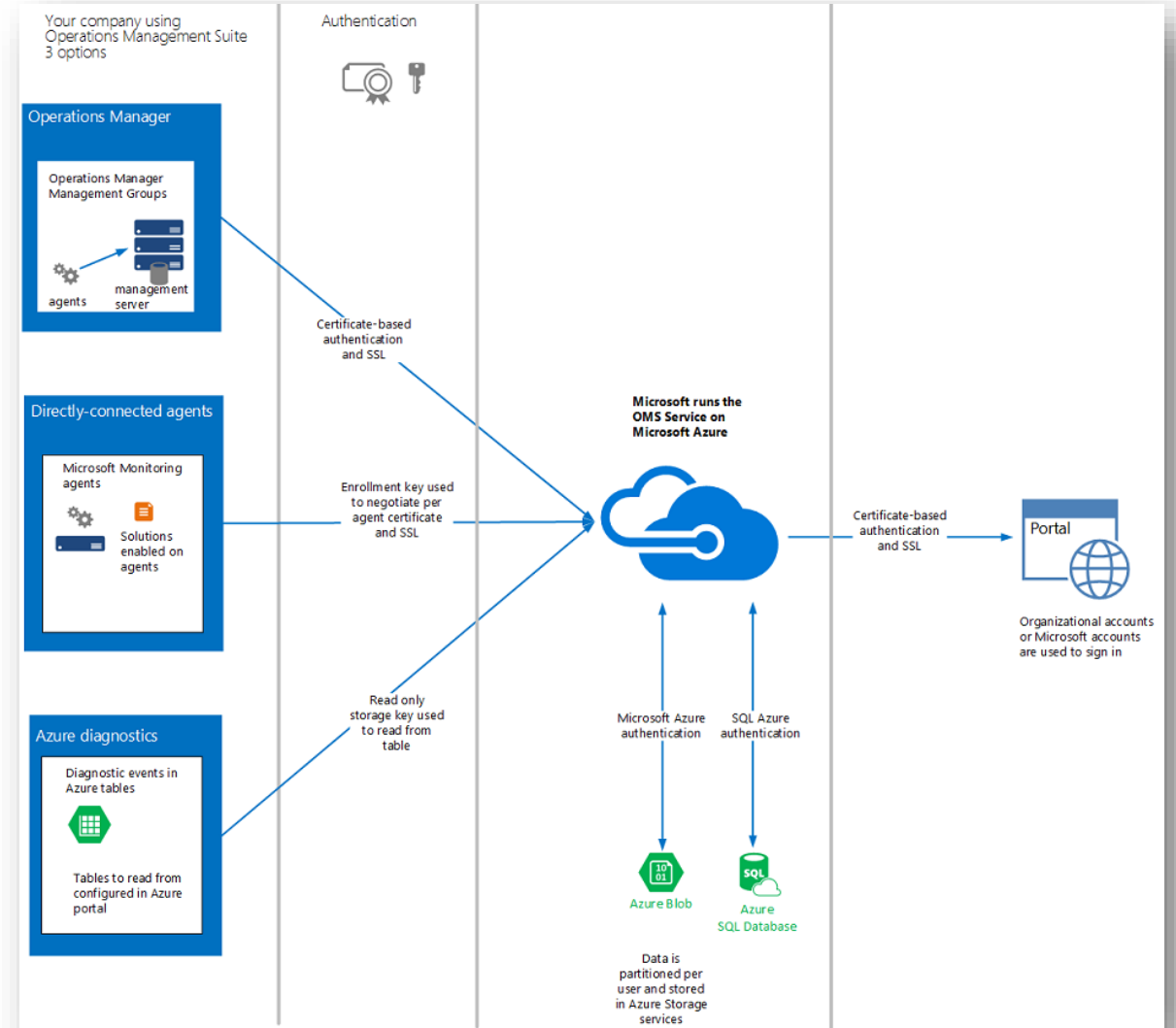
대시보드에서 결과를 시각화



내장된 인텔리전스

# Log Analytics

- 인프라 및 응용프로그램의 로그를 근 실시간으로 수집, 집계하여 운영을 위한 통찰력을 제공하는 서비스
- Microsoft 에서 운영하는 솔루션 서비스
  - ✓ Microsoft의 IT 관리 솔루션으로 System Center의 클라우드 서비스 형태로 이해할 수 있음
  - ✓ Azure 기반으로 서비스가 운영되며, Microsoft가 서비스의 가용성 및 기능에 대한 유지 관리 수행
  - ✓ 온-프레미스 또는 공용 클라우드(Microsoft Azure, AWS) 에 상관없이 사용 가능

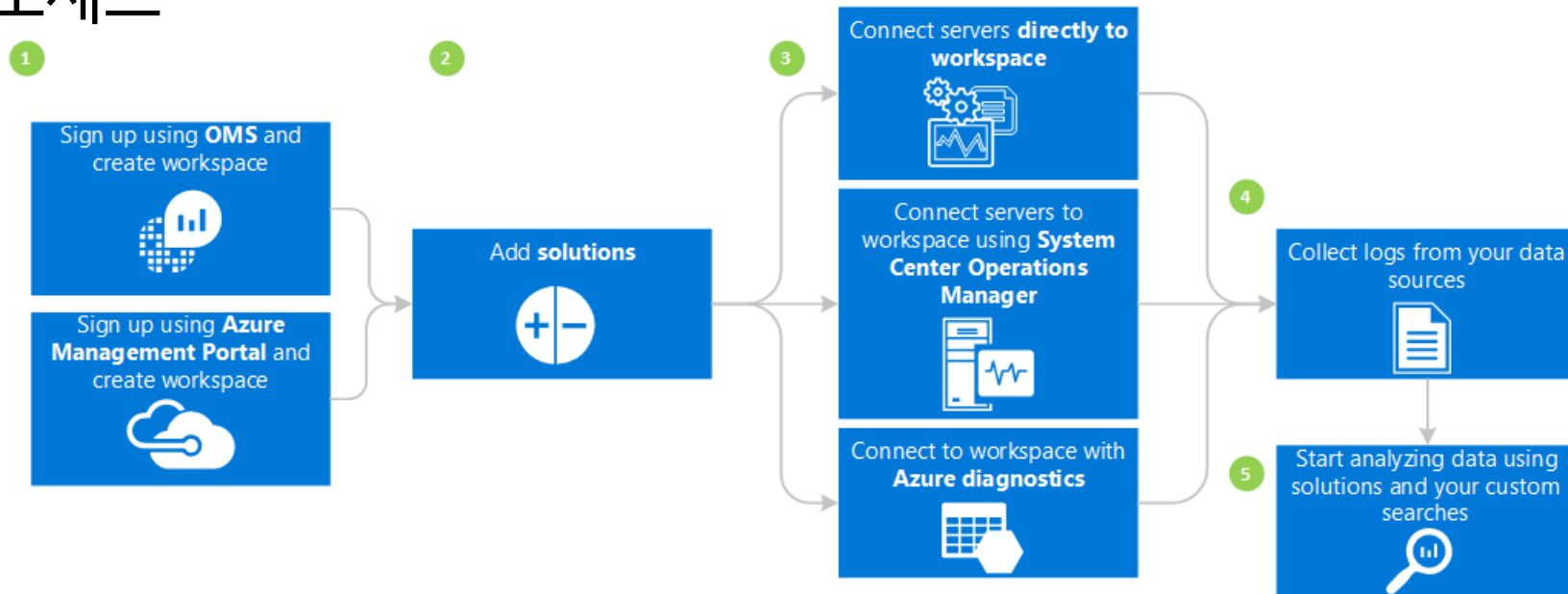


# Log Analytics - 장점

- 클라우드 서비스(SaaS)이기 때문에 초기 환경 구성 및 서비스 관리 부담이 없으며, 항상 최신의 통찰력과 솔루션을 활용할 수 있음
- 하나의 서비스에서 통합하여 기존 온-프레미스 인프라와 클라우드에 구성된 인프라를 한 화면에서 관리 가능
- 분석을 위한 로그 수집을 위한 스토리지 관리 및 데이터 관리 노력을 최소화 할 수 있음
- 수십만 로그 분석을 몇 초 내 빠르게 분석이 가능한 고성능 서비스 제공
- 관리를 위한 권장 사항과 구체적인 정보를 Microsoft Knowledge Data를 기반으로 제공
- Windows와 Linux에 모두 운영체제 수준의 관리, (10초 주기) 성능 수집 및 분석이 가능

# 서비스 구성 및 환경 설정

## • 설정 프로세스



Workspace 생성

솔루션 선택

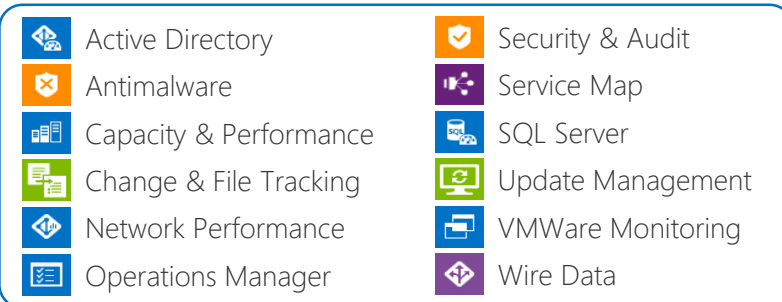
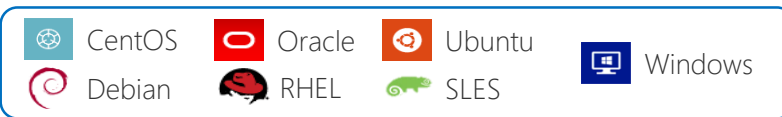
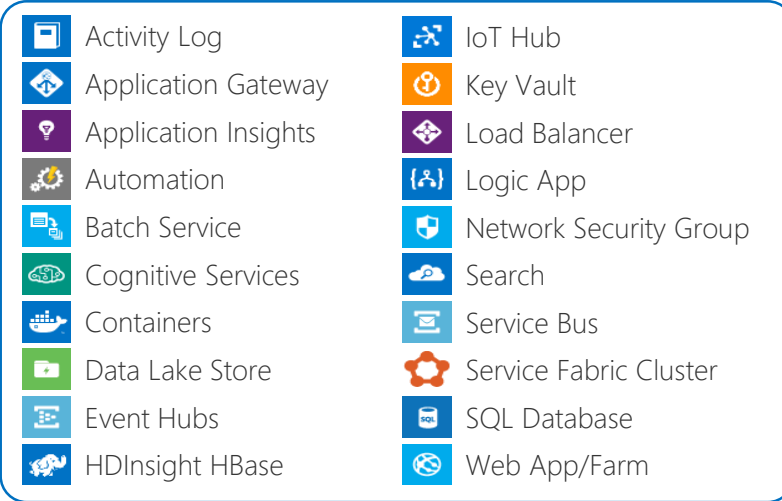
데이터 수집

- OMS Agent
- SCOM
- Azure Blob
- AWS S3

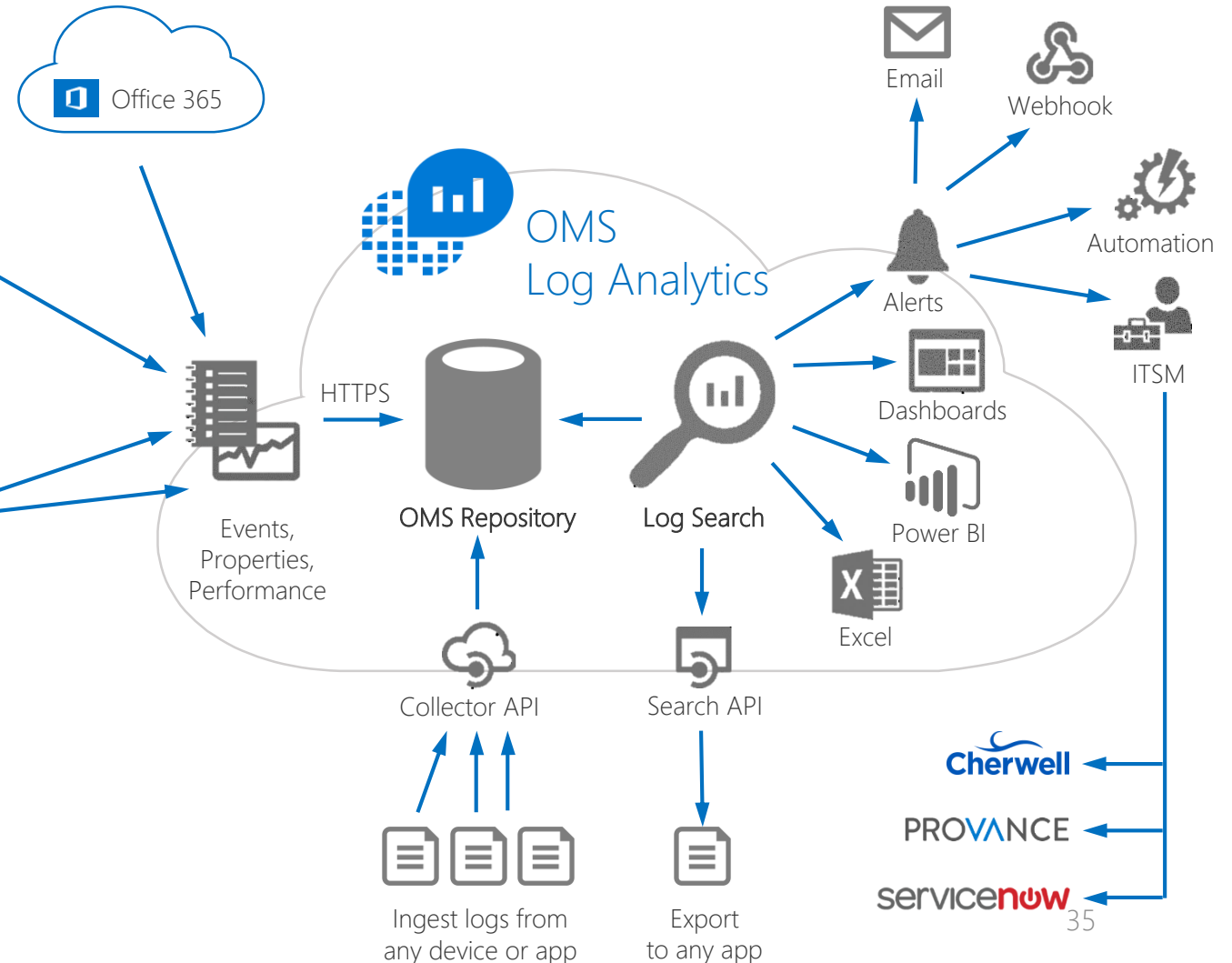
솔루션 별 분석  
및 활용

# Log Analytics

Azure



Hybrid,  
On-  
Premises,  
Any Cloud

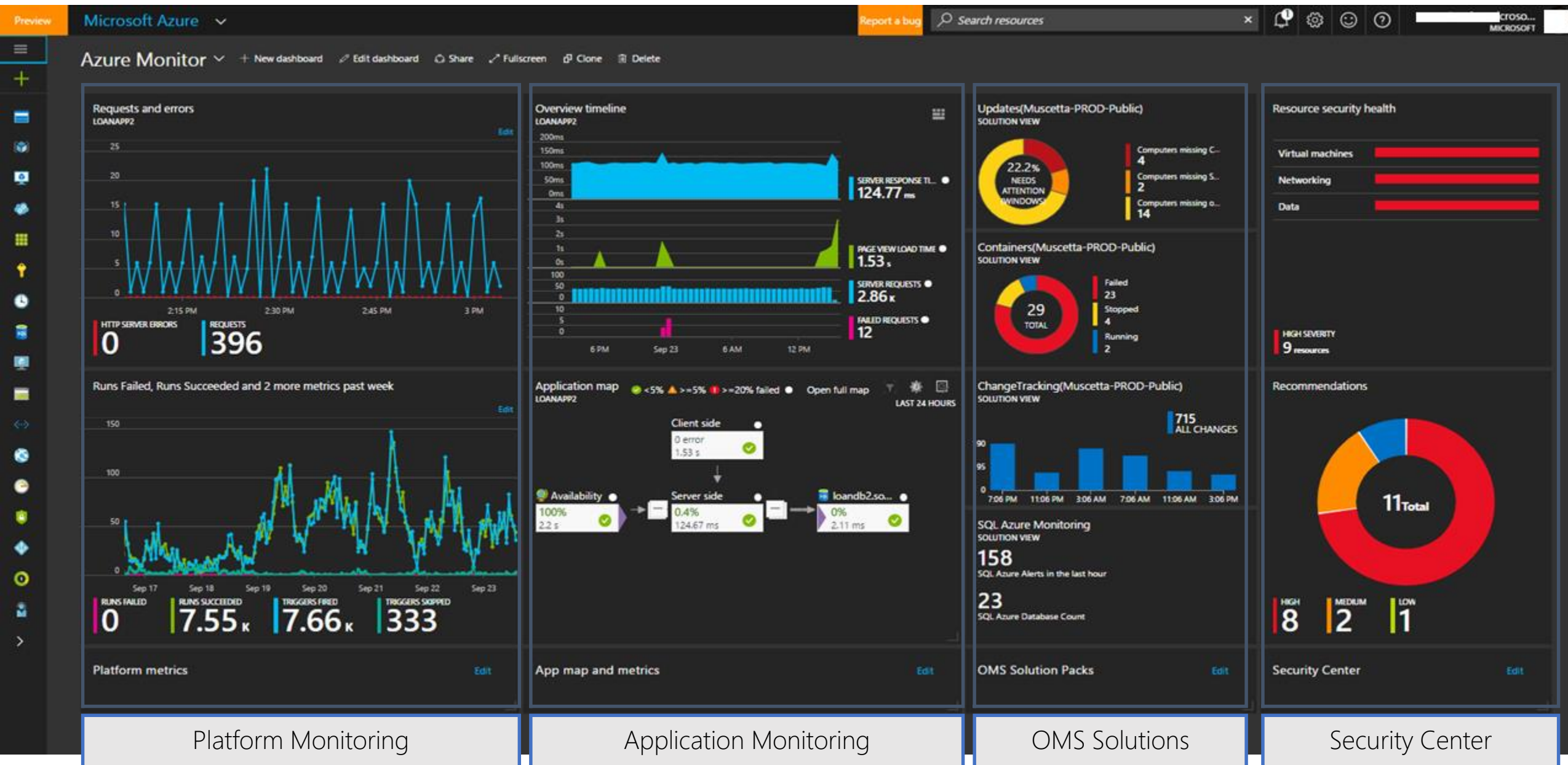


# 세션 요약

- Azure Service Health : 고객에 영향을 줄 수 있는 Azure 서비스에 대한 가이드 및 지원 제공
- Azure Monitor : 고객이 필요로 하는 세분화된, 최신 모니터링 데이터를 단일 위치에서 제공
- Log Analytics(OMS) : 온-프레미스, Azure 및 3rd party 클라우드에 대한 전체적 로그 수집 및 분석 제공

# One Dashboard

- 단일 위치에서 모든 것을 모니터링
- Azure Monitor, App Insights & OMS Log Analytics 로부터의 데이터 기반
- 대시보드를 공유하거나 복제





# Service Health

- 고객에 영향을 줄 수 있는 Azure 서비스에 대해 가이드 및 지원 제공



상태 알림

타게팅된 알림 설정



개인화된 상태  
대시보드

개인화된 대시보드에  
접근 제공



문제 관리

상세정보 및  
업데이트를 손쉽게  
공유



가이드 및 지원

가이드 및 지원 받기

# 모니터

- 모든 Azure 리소스에 대해 매우 세분화되고 근실시간으로 제공되는 모니터링 데이터

고객이 필요로 하는 세분화된, 최신 모니터링 데이터를 단일 위치에서 확인



모든 고객 모니터링  
데이터를 손쉽게 확인  
및 관리



경고 설정 및  
자동화된 조치 수행



운영 이슈를  
신속하게 진단



고객의 기존 도구와  
연동

# Log Analytics(OMS)

- On-premise, Azure 및 3rd party 클라우드에 대한 전체적 관리 제공



## Insights and Analytics

OS 및 어플리케이션  
으로 부터의  
성능/특정 데이터

Log Analytics 기능 포함



## Protection and Recovery

Azure Backup 및 Azure  
Site Recovery와 연동



## Automation and Control

Hybrid runbook worker  
그래픽기반 workbook  
제작(authoring) 및  
Automation DSC



## Security and Compliance

말웨어 평가  
보안 태세 및 시스템  
업데이트 평가

# 또 다른 모니터링 서비스는

- Azure Advisor : Azure 리소스에 대해 사전예방적 최적화를 돕는 서비스
- Azure Network Watcher : 네트워크 시나리오 레벨에서 Azure 내부, 안팎 조건에 대해 진단
- Azure Security Center : Azure 리소스에 대한 위협을 방지/탐지/대응하기 위한 기능 제공
- Azure Application Insights : 가상머신 및 App Service와 같은 PaaS 서비스의 어플리케이션 레이어를 탐지 및 진단함
- Azure Cost Management : Azure 및 타사 클라우드 리소스를 가장 잘 활용하고, 관리할 수 있도록 하는 멀티 클라우드 비용 관리 기능을 제공